RAPID7

Key Takeaways from the 2024 Attack Intelligence Report

The cybersecurity world has changed. Since the end of 2020, Rapid7 has tracked huge upticks in zero-day exploitation, ransomware attacks, and mass compromise incidents impacting many organizations worldwide. Adversary behavior has evolved, with both state-sponsored attackers and ransomware groups leveraging complex zero-day exploit chains and novel persistence mechanisms. With attack surface area continuing to grow across global cloud and on-premise environments, organizations are more pressed than ever to make security a core part of their business strategy.

Below are some key findings from Rapid7's 2024 Attack Intelligence Report.

Zero-days and network edge device exploitation

For the second time in three years, more mass compromise incidents arose from zero-day vulnerabilities than from n-day vulnerabilities. This means that many attacks are occurring before organizations even know they are vulnerable. We've also seen a shift in the way these mass compromise events are executed. Instead of following the familiar pattern of "many attackers, many targets," nearly a quarter (23%) of widespread threat CVEs arose from well-planned, highly orchestrated zero-day attacks in which a single adversary compromised dozens or hundreds of organizations, often using proprietary exploits or backdoors.

The number of large-scale compromises resulting from exploitation of network edge devices nearly doubled in 2023, with 36% of widely exploited vulnerabilities Rapid7 tracked occurring within network edge tech. 60% of these were zero-days. Network edge technologies are essential for the operation of many modern networks, but they also represent a significant weak spot in our collective cybersecurity defenses, as years of exploitation have demonstrated.

Ransomware is big business

Ransomware payments were said to have topped $1 billion globally in 2023 — and those are just the payments we know about. Ransomware groups are making tens of millions in profits by hitting organizations with double extortion attacks.

Our analysis also showed an increase in "smash-and-grab" attacks targeting file transfer solutions. In these attacks, adversaries sought to quickly gain access to sensitive data and perform exfiltration as quickly as possible. While most ransomware incidents Rapid7 observed were still "traditional" attacks where data was encrypted, smash-and-grab extortion is becoming more common.

Rapid7 Labs tracked more than

5,600 ransomware incidents

reported between January 2023 and February 2024. That number is likely to be much higher in reality, since many ransomware attacks still go unreported.

MFA is still a gap for many organizations

VPNs and virtual desktop infrastructure were the leading targets of incidents that could have been prevented or slowed down by correctly implemented MFA. Vulnerability exploitation was also a common initial access vector in incidents Rapid7 MDR responded to in 2023 and early 2024.

How can organizations protect themselves?

Implementing and enforcing multi-factor authentication should be a top priority for security teams. With 40+% of incidents stemming from a lack of MFA protections, it is the single most important fix we recommend. Being proactive and aggressive about reducing internet-exposed attack surface area is also critically important in today's threat climate.

In light of prevalent attacks on file transfer technologies, we also recommend that organizations put measures in place to more quickly identify and prevent data exfiltration. This includes monitoring or blocking known file-sharing sites or data transfer utilities, alerting on (or restricting) large file uploads and unusual access to cloud storage, and implementing egress filtering.

Finally, as always, a robust vulnerability management program is a core component of any security strategy, both in the cloud and on-prem. The importance of strong vulnerability and patch management foundations hasn't decreased as threat actors have evolved their techniques and operations — to the contrary, these fundamental practices are some of the best proactive steps organizations can take to minimize exposure to modern threats.

Additional resources

When a new threat arises, Rapid7 guidance can be found in the emergent threats section of the Rapid7 blog, along with corresponding information for Rapid7 customers. Rapid7 researchers and community members publish vulnerability analysis in Rapid7's open research platform, AttackerKB. These analyses often include sample proof-of-concept code and indicators of compromise in addition to exploitation timelines and attack chain analysis. Rapid7 zero-day vulnerability research is published on a regular basis here.

More than

40%

of the incidents Rapid7's managed detection and response teams saw in 2023 stemmed from missing or unenforced multi-factor authentication (MFA).

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management

Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight